



eHI Blueprint: Building Consensus for Common Action

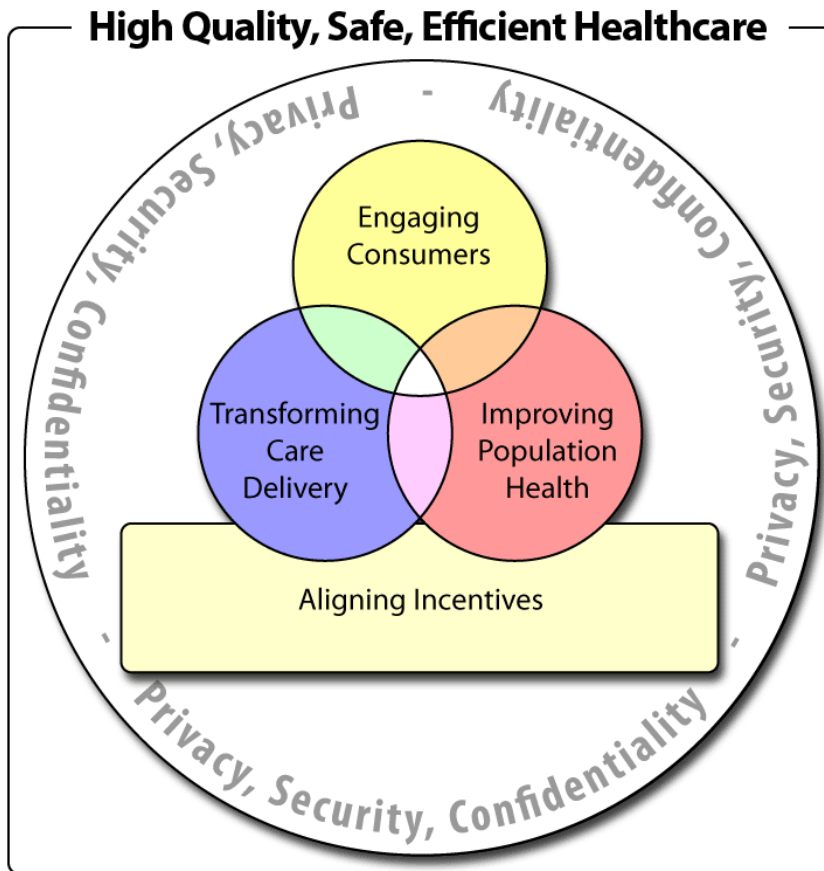
MANAGING PRIVACY, SECURITY AND CONFIDENTIALITY

- **Introduction to Managing Privacy, Security and Confidentiality**
 - Principles for Managing Privacy, Security and Confidentiality
 - Overview of Common Core Questions
 - Discussion/Questions and Answers
 - Co Chairs: Robert D. Marotta, Senior Vice President and Regulatory Counsel, HLTH Corporation; Treasurer, eHealth Initiative and Foundation and Mark Frisse, MD, Director, Regional Health Initiatives, Vanderbilt Center for Better Health
- **From Consensus to Common Action: What You Can Do**
 - Discussion
 - Co Chairs: Robert D. Marotta, Senior Vice President and Regulatory Counsel, HLTH Corporation; Treasurer, eHealth Initiative and Foundation and Mark Frisse, MD, Director, Regional Health Initiatives, Vanderbilt Center for Better Health
- **Wrap Up – Next Steps**
 - Co Chairs: Robert D. Marotta, Senior Vice President and Regulatory Counsel, HLTH Corporation; Treasurer, eHealth Initiative and Foundation and Mark Frisse, MD, Director, Regional Health Initiatives, Vanderbilt Center for Better Health

- High-performing healthcare system where:
 - **All those engaged in the care of the patient are linked together in secure and interoperable environments,**
 - **The decentralized flow of clinical health information directly enables the most comprehensive, patient-centered, safe, efficient, effective, timely and equitable delivery of care [1]**
 - **Where and when it is needed most – at the point of care.**

[\[1\]](#) Institute of Medicine, 2001.

Our Shared Vision



In our vision, financial and other incentives are aligned to directly support and accelerate all of the key elements of transformation -- engaging consumers, transforming care delivery at the point of care, and improving population health -- in a secure, private, and trusted environment.

1. Transparency:

- Policies for the permissible use of personal health information by those other than the patient should be clearly defined, accessible, and communicated in an easily understood format.
- Individuals have the right to know how their personal health information has been used and who has access to it.

2. Collection and Use of Personal Health Information:

- Personal health information of the individual consumer should be obtainable consistent with applicable federal, state and local law. It should be accurate, up-to-date, and limited to what is appropriate and relevant for the intended use.
- Consumers have a right to privacy of their personal health information, taking into account existing exceptions under law. Consumers should be apprised when they have a choice in how their personal health information will be used and shared and when they can limit uses of their personal health information.

3. Individual Control:

- **Individuals should be able to limit when and with whom their identifiable personal health information is shared.**
- **Individuals should be able to delegate these responsibilities to another person.**
- **Individuals should be able to readily obtain an audit trail that discloses by whom their personal health information has been accessed and how it has been used.**

4. Security:

- Measures should be implemented to protect the integrity, security, and confidentiality of each individual's personal health information, ensuring that it cannot be lost, stolen, or accessed or modified in an inappropriate way.
- Organizations that store, transmit, or use personal health information should have in place mechanisms for authentication and authorization of system users.

5. Audit:

- Each such organization must have a comprehensive audit process to examine compliance with its internal privacy, security, and confidentiality policies and procedures.
- Organizations have a responsibility to ensure that an individual is notified when the organization learns of unauthorized or inappropriate access to that individual's personal health information.

6. Accountability and Oversight:

- Individuals should be apprised as to who monitors policy compliance with privacy, security and confidentiality policies, how complaints will be handled, how individuals will be informed of a violation and existing remedies available to them.

6. Technology and Privacy:

- Technological developments must be adopted in harmony with policies and business rules that foster trust and transparency.
- Privacy protections must be at the forefront of all technological standards. Privacy issues cannot be addressed post-system design and implementation.

Common Core Questions

MANAGING PRIVACY, SECURITY AND CONFIDENTIALITY

1. What federal and state privacy and security laws are you subject to? Are partner stakeholders subject to the same laws? What are the implications if stakeholders are subject to different laws?
2. There maybe differences under federal and state laws as to how different types of health information (e.g. mental health and substance abuse) are handled. What are the implications of having different laws for different types of health information?

3. What are the implications of having different federal and state laws affecting privacy and security? Is there consensus on how the laws apply to each stakeholder? What are the implications of having different laws across states?
4. Not all entities are covered by the same laws even in the situation that they perform the same services (e.g. HIPAA). What are the implications of having some entities performing similar services covered by federal law (e.g., HIPAA) and others not?
 - How does this impact your competitiveness?
 - How does this impact your ability to exchange information with others?
 - Does contracting with non-covered entities create different levels of accountability and/or enforceability in the exchange of health information?
 - Assuming you are not a covered entity or its business associate, what would be the implications of complying with enforceable confidentiality, privacy, and security requirements at least equivalent to relevant HIPAA principles?

5. Should there be different confidentiality, privacy, and security protections for electronic records as compared to paper records, whether in whole or in part?
6. Is there a minimum set of confidentiality, privacy, and security protections that you think any organization that stores, transmits, and/or uses personal health information should follow --- if not HIPAA, then what?
7. How and when should privacy and security policies be available to employees? How will employees be held accountable to following these policies?

8. How do you collect, maintain, store, share or transmit personal health information?
9. What is your approach for dealing with breaches of privacy and security?
10. How and at what point in time do you communicate your privacy and security practices to patients/consumers? How and at what point in time do you communicate changes in your practices?

Common Core Questions About Privacy and Security:

11. What level of consent and how much control are consumers given over the flow of their information, i.e., “authorization and consent,” before disclosure, “ability to review and correct information,” and so on? What level of control should consumers have over the use of de-identified patient data for population health initiatives or research that is outside the direct care delivery process? What is the best way to educate consumers about these issues and the impact of their choices?

- **Feedback and Overall Reaction**
 1. Principles
 2. Common Core Questions
- **How should we build on the Common Core Questions?**
- **What is going on now in Privacy and Security?**
- **What should eHI's role be?**